4 August 2025

# Guidance: Server Retrieval for Verifiable Credentials

## Purpose and Scope

This document provides guidance for the design and implementation of digital identity services, on the Server Retrieval Method in the context of Verifiable Credentials (VCs). It outlines what the method is, the risks it presents, its status under the Digital Identity Services Trust Framework (DISTF) in New Zealand, and an approved alternative approach.

This guidance applies to all system architects, developers, service designers, policy teams, others involved in the design or implementation of digital identity services.

## What is the Server Retrieval Method?

The Server Retrieval Method[[1]](#footnote-1) is a model of data sharing in which a verifier obtains a data contained in verifiable credential or presentation by contacting a remote server usually operated by the credential’s issuer rather than receiving the data directly from the user via their device at the time of credential presentation.

Typically, the user provides the verifier with a URL or token that allows access to the credential or presentation stored on a hosted endpoint.

## Risks and Limitations

The Server Retrieval Method introduces several privacy, security, and architectural concerns:

### Privacy Risks

Verifiers may reveal credential use to third parties, allowing the server’s operator to observe who is verifying what and when.

It increases the risk of users being tracked or profiled based on their credential usage.

### Loss of User Control

The user is not always actively involved in the presentation process once the server link or token is shared.

This undermines consent, as the verifier may be able to request the credential without the user’s knowledge.

### Reliance on Centralised Infrastructure

The availability of the credential or presentation depends on the issuer’s server(s) being online and functional.

### Security and Disclosure Risks

Without strict access controls and anti-replay protections, there are new design-level risks introduced such as credential misuse, replay attacks, and privacy violations, including from malicious actors.

## Trust Framework Position on Server Retrieval

Under the Digital Identity Services Trust Framework (DISTF) in New Zealand, the Server Retrieval Method is not permitted when presenting credentials by accredited facilitation services.

The framework requires that digital identity services uphold principles of:

* User control over when and how their information is shared.
* Privacy, including data minimisation and preventing unnecessary correlation.
* Interoperability, without relying on centralised infrastructure at the time of presentation.

Because the Server Retrieval Method fails to meet these principles, its use by accredited facilitation services is explicitly prohibited in the Trust Framework Rules.

## Recommended Alternative: Device Retrieval

The preferred model is a user-mediated presentation, known as Device Retrieval,[[2]](#footnote-2) where the user presents their credential directly to the verifier, without reliance on the issuer’s servers during presentation.

Key characteristics of this method:

* The user initiates and consents to the data sharing.
* The presentation occurs in a peer-to-peer or device-to-device manner, often using secure protocols or physical interactions.

This approach supports both online and offline use cases, including through:

* Bluetooth, NFC, or Wifi Aware transfer.
* App-to-app data exchange.

## Supporting Standards

The Device Retrieval method is supported and standardised in multiple recognised specifications, including:

* ISO/IEC 18013-5: Defines secure device-to-device data retrieval (e.g., via NFC, Bluetooth, or Wifi Aware) for offline and consent-based credential presentation.
* ISO/IEC 18013-7: Includes conformance profiles for offline and online device retrieval methods, as well as guidance for interoperability testing.
* OpenID for Verifiable Presentations (OID4VP): Defines presentation flows that allow credentials to be shared directly from the user’s wallet app to a verifier’s application, over secure and user-consented protocols.
* DIDComm v2 Protocol: Used in decentralised identifier systems for secure, peer-to-peer messaging and credential exchange.

## Summary Comparison

| Feature | Server Retrieval | Device Retrieval |
| --- | --- | --- |
| **Privacy** | Higher risk of data correlation | Protects user privacy |
| **User control** | Limited | Full user control |
| **Consent** | Required at time of use | Required at time of use |
| **System availability** | Server-dependent | Works online or offline |
| **DISTF compliance** | Not permitted | Recommended |
| **Decentralisation** | Centralised infrastructure | Peer-to-peer |

## Implementation Expectations

All services and applications developed within the Trust Framework ecosystem should:

* Avoid using server retrieval methods for verifiable credentials or presentations.
* Use device retrieval presentation models in all credential exchanges, ensuring user consent, privacy, and control are maintained.
* Design systems to operate without centralised servers during the credential verification process.
* Any deviation from this guidance is unlikely to meet compliance requirements under DISTF.

1. Including as defined in ISO 18013-5:2021 - 9.2 Server Retrieval [↑](#footnote-ref-1)
2. Including as defined in ISO 18013-5:2021 – 9.1. Device Retrieval [↑](#footnote-ref-2)